PATENT APPLICATION
Docket No.: 13768.154

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of		)
		)
	Michael Kramer, et al.	)
		)
Serial No.:	09/768,673	) Art Unit
		) 2137
Conf No.:	3903	)
		)
Filed:	January 24, 2001	)
		)
For:	ESTABLISHING A SECURE CONNECTION	)
	WITH A PRIVATE CORPORATE NETWORK	)
	OVER A PUBLIC NETWORK	)
		)
Examiner:	Courtney D. Fields	)
		)
Customer No.:	047973	)

DECLARATION UNDER 37 C.F.R. § 1.131 OF MICHAEL KRAMER

I, Michael Kramer, declare as follows:

1. I am a co-inventor of the invention claimed in the above-identified patent application. During the period that the invention claimed in the above-identified patent applications was conceived and reduced to practice, I was a vendor under contract with Microsoft Corporation, the assignee of the above-identified patent application, to develop architectures and designs for mobile and remote information access including those related to the invention claimed in the above-identified patent application.

2. During my vendor relationship with Microsoft Corporation, and prior to December 13, 1999, I (along with my co-inventors) conceived the concepts for establishing a secure connection with a private corporate network as described and claimed in the above-identified patent application.

3. Attached as Exhibit A is a copy of a PowerPoint Presentation document entitled "Airstream Security" dated December 13, 1999 (hereinafter referred to as the "First PPT Document"), which includes overview descriptions of the concepts of establishing a secure connection in accordance with the invention.

4. Attached as Exhibit B is a copy of a PowerPoint Presentation document entitled "Airstream" dated December 23, 1999 (hereinafter referred to as the "Second PPT Document"), which includes a more detailed description of the concepts of establishing a secure connection in accordance with the invention.

5. I was personally involved with the conception and reduction to practice of the concepts relating to establishing a secure connection described in the First PPT Document and the Second PPT Document.

6. The Second PPT Document was last modified on December 23, 1999.

7. Although the Second PPT Document was last modified on December 23, 1999, the concepts supporting the substance of the concepts of establishing a secure connection in accordance with the invention were already conceived of before December 13, 1999 as represented in prior versions of the Second PPT Document, which prior versions have been superceded by the final version of the Second PPT Document, and which prior versions are not readily available.

8. Immediately following conceiving of the concepts of establishing a secure connection in accordance with the invention, I began diligently working with employees of Microsoft Corporation for the purpose of actually reducing the concepts to practice.

9. No later than April 21, 2000, working code was authored by such employees, the working code functioning using the general principles that I communicated to them regarding the concepts of establishing a secure connection in accordance with the invention;

10. Between the dates of December 13, 1999 and April 21, 2000, continuous efforts were being made either by myself, or by others within Microsoft Corporation, to move forward towards authoring such working code.

11. I declare further that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful, false statements may jeopardize the validity of the application or any patent issuing thereon.

Dated this 18 day of May 2006.

Inventor: Michael Kramer

Michael Kramer
29 Fanshaw Avenue
Yonkers, New York 10705
United States

EXHIBIT A

AIRSTREAM

Airstream Security

Mike Kramer, Airstream Program Manager

Microsoft® Mobile Internet

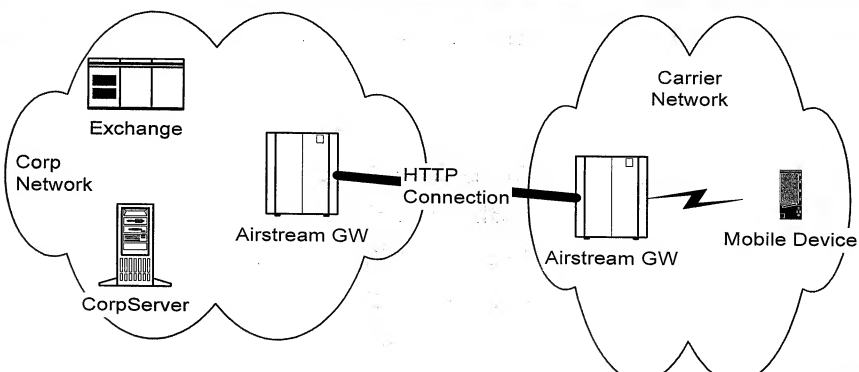
Overview

AIRSTREAM

- Not a new protocol
  - Airstream implements a protocol stack built around HTTP and friends
    - Some protocol enhancements for security and perf
    - One new protocol for running HTTP over SMS
- Airstream provides
  - Secure Push mode messaging
  - Secure end-to-end Browse mode communications

Network Overview

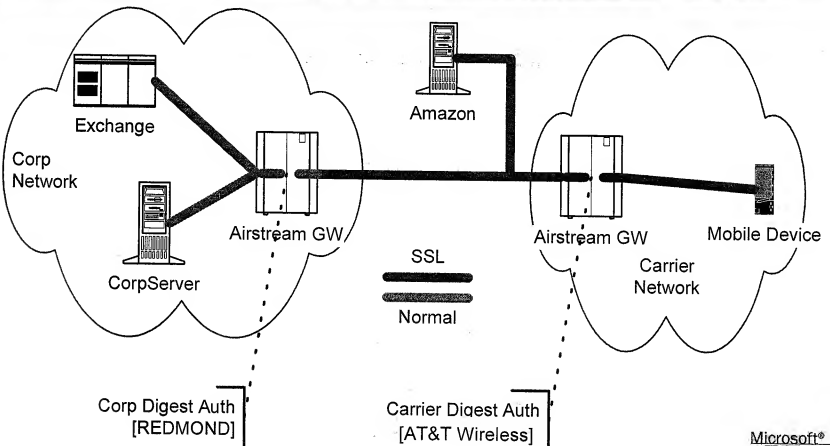
AIRSTREAM



Microsoft® Mobile Internet

Browse Topology

AIRSTREAM



Microsoft® Mobile Internet

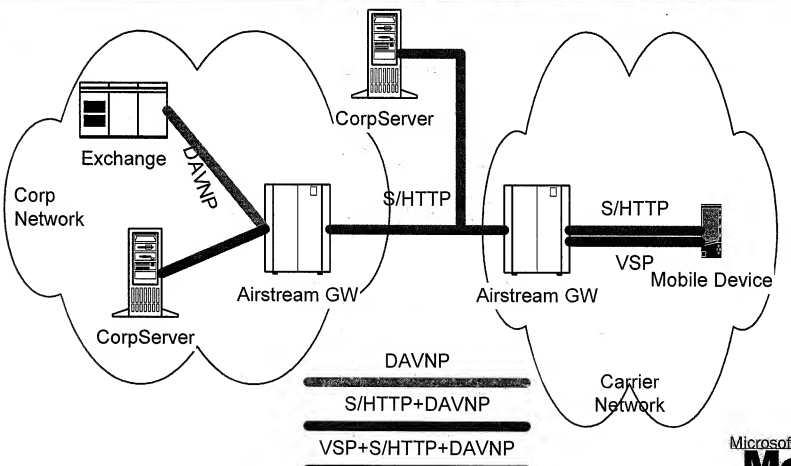
Push Overview

AIRSTREAM

- Messages are communicated via DAV-NP
  - DAV-NP = GENA = HTTP
- Session keys are established a priori with the Key Negotiation Protocol (KNP)
- Messages are encrypted with KNP session key set up by client device (S/HTTP)
- Auth only mode uses Digest

Push Topology

AIRSTREAM



Microsoft® Mobile Internet

Key Technologies

AIRSTREAM

- Digest Authentication
- SSL
- VSP – Virtual Session Protocol
- KNP – Key Negotiation Protocol
- S/HTTP
- Compression (optional)

SSL

AIRSTREAM

- Well known connection level encryption
- Currently not using client certs
  - SSL Provides encryption only
- Long lived Session key
  - SSL Session resume
- SSL can be used with various ciphers
  - RSA
  - ECC

VSP

AIRSTREAM

- Very Light weight Session protocol
- Provides
  - Segmentation / Reassembly of HTTP
    - Many SMS systems do not provide this
  - MUX for multiple sessions

Key Negotiation Protocol

AIRSTREAM

- Based on HTTP w/ Extension framework
- Defines a new method and header
- Run over SSL connection
- Client periodically refreshes Push Session key
- Server can invalidate key as well
  - Server crash
  - Known compromise

Microsoft® Mobile Internet

S/HTTP

AIRSTREAM

- Provides object level encryption for HTTP messages
- Actually a "variant" of experimental S/HTTP protocol optimized for wireless
  - Uses session keys instead of PKI which is much cheaper
- HTTP messages are enveloped in another HTTP (S/HTTP message)

Compression

AIRSTREAM

- GZIP
  - Well known compression algorithm
  - Used for Push, device decompresses
  - Especially helpful when encryption is used
- Tokenization
  - A work in progress in W3C
  - Possible use for V2+

Microsoft® Mobile Internet

EXHIBIT B

Airstream

Marc Seinfeld (marcse)
Michael Kramer (v-mikekr)
Josh Cohen (joshco)

What are we trying to accomplish?

Airstream V1 provides Knowledge Workers

Secure access to their Email and PIM

Anywhere, Anytime, on any device

Broader Airstream Wave Roadmap:

Access "on the go" for Knowledge Workers and Consumers to Email, Contacts, Calendar, Tasks and other critical information on their "Digital Dashboard"

Enable Secure Mobile Access to Content

- Initial target: Exchange data
  - Corporate mission critical personal information
- Also: Origin Web Servers on Intranet
  - Becoming strategic necessity for mobile worker
- Also: Origin Web Servers on Internet
  - Enhanced information access for professional and personal needs

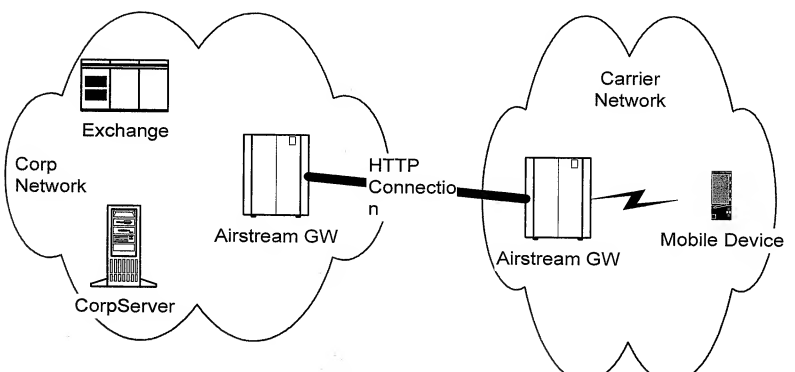
AirStream Program

- Develop a server product for carriers and corporations
- Launch a developer program to allow 3rd party products on platform and new devices
- Work with client device platforms – MME, Win CE and RIM pagers
- Conduct trials with carriers, multi-carrier service providers and information service providers

Mobile Access: New Two-Tier Server Architecture

- Carrier or Service Center:
  - Offer Mobile Internet access and portal services
  - Serve as an "ASP" for mobile access to secure Corporate data
  - Pay CAL and/or SAL licensing fees
- Corporation:
  - Manage and maintain corporate data and corporate Intranet
  - Allow controlled secure access to Intranet through firewall
  - Continue to license OS and Exchange as previously

Network Overview



Mobile Access: New Application for a New Market

- New Web Component:
  - Web Proxy Acting Like a VPN Server
  - Content Transformations for Registered Devices
  - "Push" Alert Server
  - Serve non-IP devices
- New Customer Segments:
  - Add: Carriers, NOC's, InfoService Providers

Mobile Access: New Application for New Devices

- Enable Access for Devices:
  - Laptops
  - PalmPC
  - Phone
  - Pagers

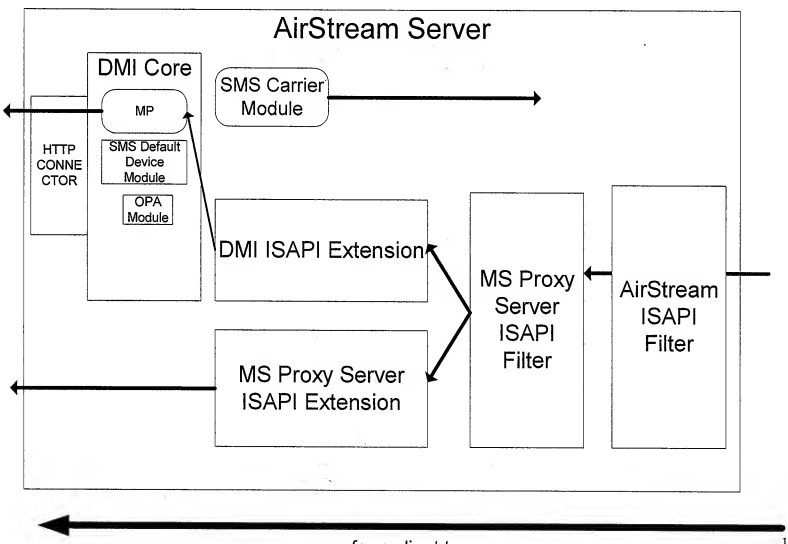
Interactive Mobile Access: New Technical Requirements

- Use existing Internet protocols – "GOI" not WAP
- NOC based authentication (NOC credentials)
- Privacy between device and NOC
- Corporate based authentication (Corporate credentials)
- Privacy between device and corporate server
- Need lightweight protocols – limited devices and networks that offer slow speed and high latency
- Support for end-to-end device access to existing Intranet Origin Web Servers using SSL

Mobile Access: New Technical Requirements

- Allow non-IP devices to access
- Allow devices to be labeled, registered and recognized
- Perform device-specific transformations on content
- Allow user to set preferences for further customization
- Serve as an alert server to allow applications to "push" information to devices using SMS or other data channels

V1 AirStream Architecture



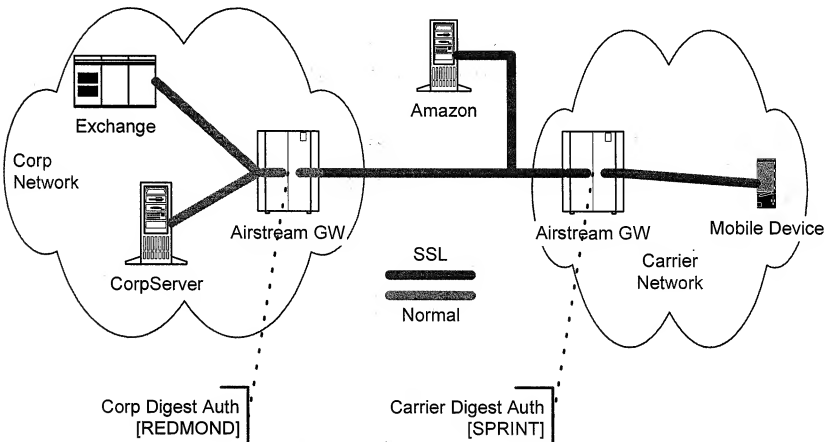
AirStream Server Architecture

SERVICE/Transport	Pass-thru	Message based "Value Add"
REQUIRED FUNCTIONS	• SSL / HTTP VPN –Privacy –Authentication • HTTP Routing • NOC to Corporate Connectivity	• Content Filter: –Device Rendering –Content Adaptation –Aggregate Retrieval •DAV-NP Push Gateway •Protocol Translation to/from IP –Mobitex –SMS
MODULE (Supplying the Function)	AirStream ISAPI's plus MS PROXY SERVER (Formerly: DMI)	DMI

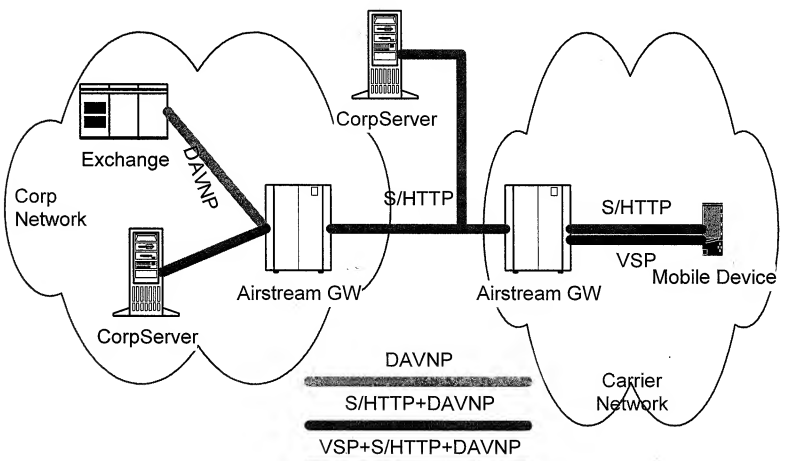
Browse Overview

- Device communicates over HTTP
  - Device acts like a Web Browser
  - Airstream acts as a Secure Proxy
- Authentication is Digest Authentication
  - Standardized HTTP Authentication mechanism
  - In IE5, IIS, Apache
- Encryption is with SSL
  - Persistent SSL sessions (cached)
  - Choice of cipher (RSA/ECC)
  - We support:
    - Terminal to GW (WTLS parity)
    - End to End (classic SSL)– better than current WAP

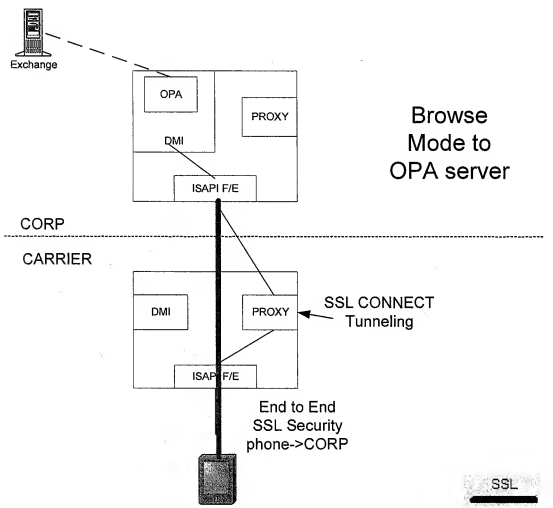
Browse Topology

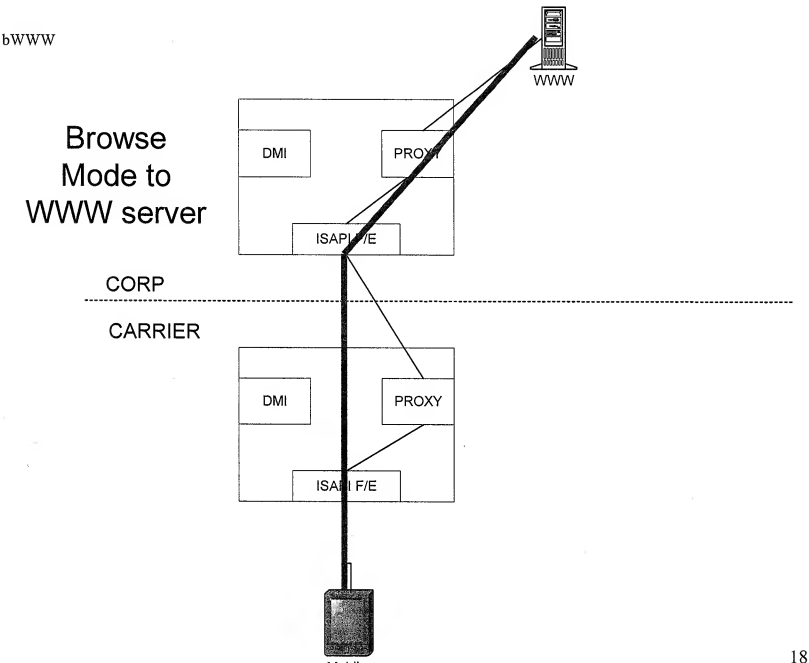


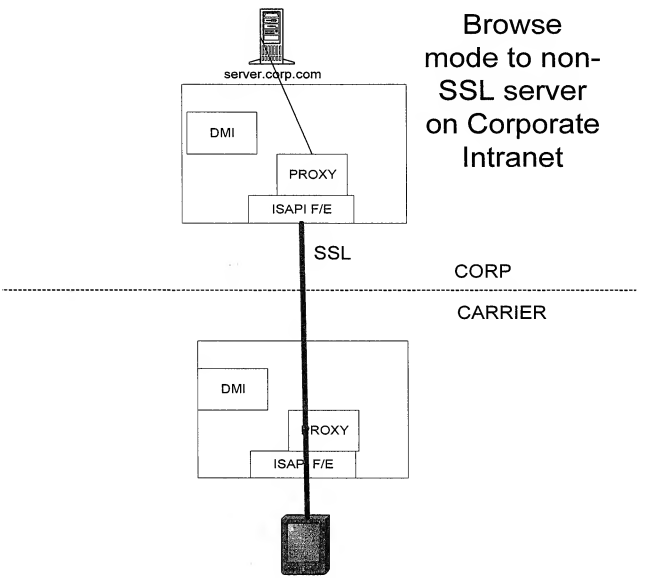
Push Topology



Scenarios

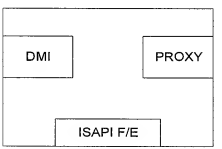

Exchange
OPA
PROXY
DMI
ISAPI F/E
Browse
Mode to
OPA server
CORP
CARRIER
DMI
PROXY
SSL CONNECT
Tunneling
ISAPI F/E
End to End
SSL Security
phone->CORP
Mobile
SSL


Browse
Mode to
WWW server
WWW
DMI
PROXY
ISAPI F/E
CORP
CARRIER
DMI
PROXY
ISAPI F/E
Mobile



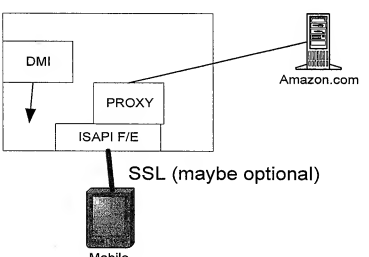
Browse mode to non-SSL server on Corporate Intranet

Browse mode to non-SSL server on Internet

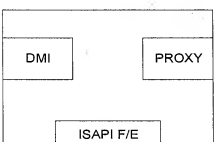


CORP

CARRIER

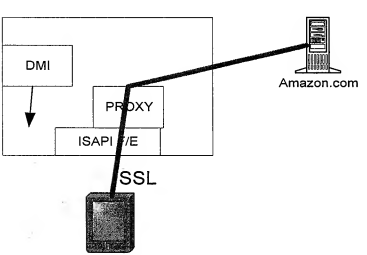


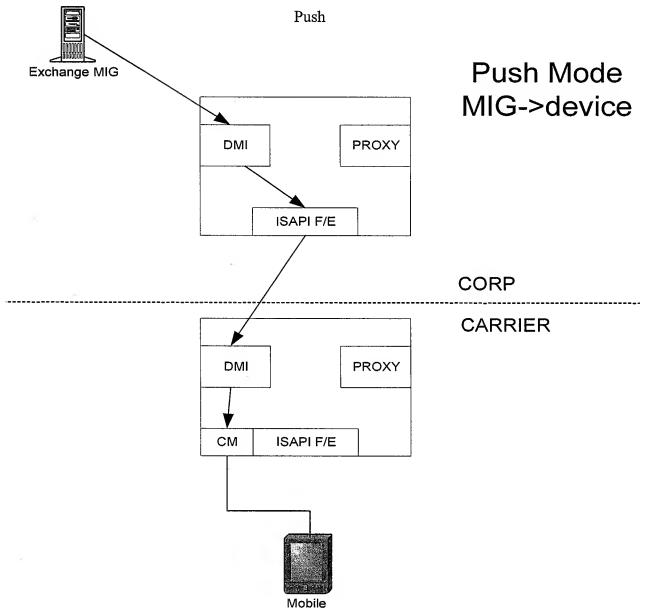
Browse mode to SSL server on Internet



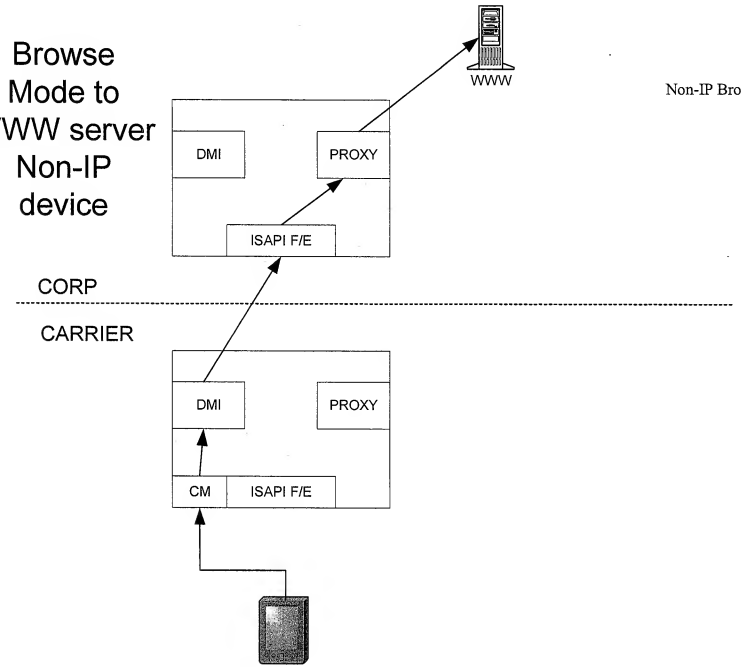
CORP

CARRIER




Push
Exchange MIG
Push Mode
MIG->device
DMI
PROXY
ISAPI F/E
CORP
CARRIER
DMI
PROXY
CM
ISAPI F/E
Mobile

Browse Mode to WWW server Non-IP device



Non-IP Browse

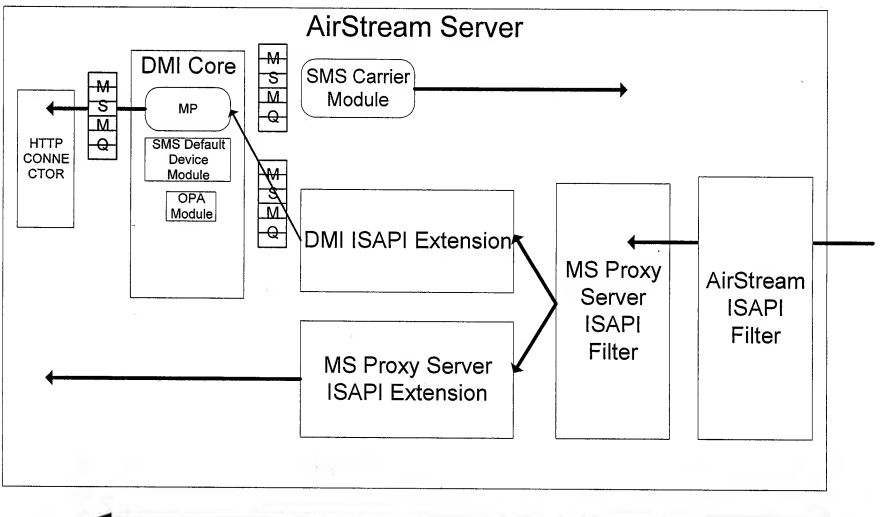
AirStream Proxy Enhancements

- Proxy SSL Front End
- Multi-Hop Proxy-authentication
- SSL Resume
- Delegated Digest

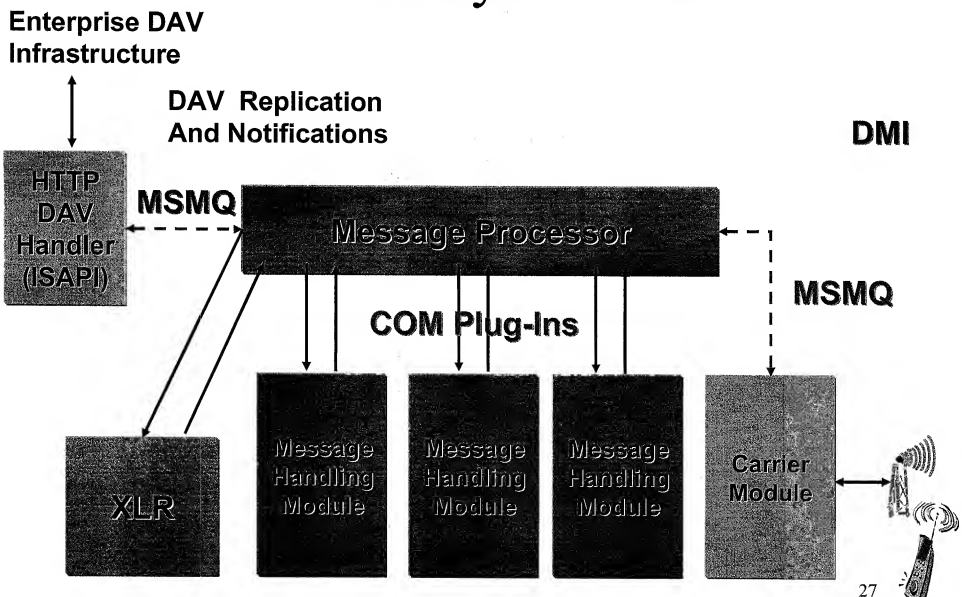
AirStream Does Not Use:

- Caching features
- Winsock Proxy
- SOCKS Server feature
- Others…
- (Will use reverse proxy)

V1 AirStream Architecture



DMI Gateway Architecture



AirStream Server Architecture

SERVICE/Transport	Pass-thru	Message based "Value Add"
REQUIRED FUNCTIONS	• SSL / HTTP VPN –Privacy –Authentication • HTTP Routing • NOC to Corporate Connectivity	• Content Filter: –Device Rendering –Content Adaptation –Aggregate Retrieval •DAV-NP Push Gateway •Protocol Translation to/from IP –Mobitex –SMS
MODULE (Supplying the Function)	AirStream ISAPI's plus MS PROXY SERVER (Formerly: DMI)	DMI

Productization Issues – TB Solved

- Bundling and Packaging
- Positioning
- Functionality
- Installation
- User Interface – Which MMC plug ins and how?

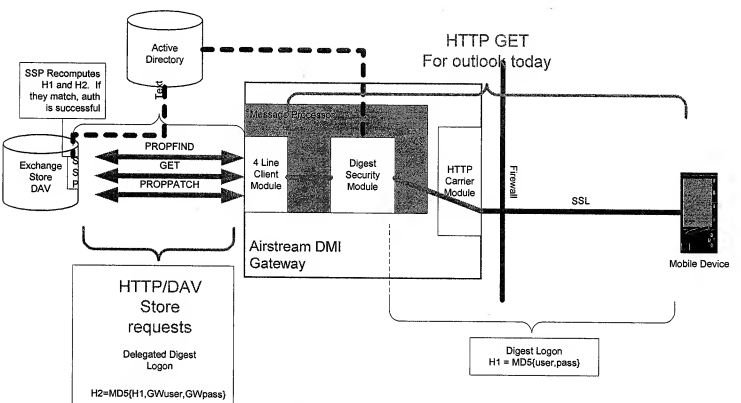
AirStream Security Feature: Delegated Digest

Delegated Authentication

Airstream is acting on behalf of the user

- How does exchange **know** that request is from the user, not Airstream impersonating at will?

Solution – Establish E2E auth between Device and Exchange

- Device signs request
- Airstream forwards signed request
  - Airstream proves it is legitimate forwarder

Delegation Topology